REMARKS

By this amendment claims 1-47 and 50-58 remain in the application reconsideration of which is respectfully requested in view of the following remarks. Claims 48,49 and 59-61 are canceled. Amendment has been made to claims 11-16 so that terms therein comport more precisely with expressions in Claim 1 from which they depend.

The Final Office Action has rejected claims 1-10, 12, 13, 15-18, 20-41, 43, 44, 47-49, 51, 52, and 57-59 under 35 U.S.C. 102(e) as being anticipated by Warren, U.S. Patent No. 5,963,909. This rejection is respectfully traversed. In order for the Office Action to establish a proper rejection under 35 USC 102 the Office Action must establish a prima facie case of anticipation by showing that all elements of the claim are fully met by the cited reference.

Claim 1 is directed to a data transfer apparatus for secure transfer of a plurality of data blocks. The apparatus comprises an encryption key generator for providing an encryption key assigned to each single data block of the plurality of data blocks and a block synchronization index indicating a correspondence between said encryption key and said single data block. In citing Warren the Office Action appears to be equating the equivalence of the tags used by Warren for preventing reproduction of a multimedia signal with the block synchronization index taught and claimed by applicant. In this regard the Office Action refers to Warren and column 9, lines 40-48 as alleged support for the Office Action's position. It will be noted that the discussion in column 9 pertains to an embodiment of Figures 3 and 4 wherein there is no encryption of the multimedia data. Yet there are provided the various tag encodments that are used for different purposes from encryption. Now since the embodiment of Figures 13-15 do use these tags as well as encryption it is submitted to be clear that these tags in no way comprise a block synchronization index indicating a correspondence between the encryption key and a single data block because they exist independently of any encryption. For this reason it is respectfully submitted that the Office Action has failed to establish a prima facie case of anticipation.

With regard to Claim 3, this claim is a dependent claim of Claim 1 and is directed to and further limits the claim to wherein the size of said single data block is further conditioned by an offset value. The Office Action has provided no reason that Claim 3 is anticipated by Warren which provides no discussion of this feature and it is submitted therefore that the Office Action has failed to establish a prima facie anticipation of this claim. The use of the offset value as disclosed in the application provides for, for example, the use of variable size data blocks which provides for enhanced security.

Claim 20 is an independent claim directed to a method for secure transfer of a data stream from a digital data source to a digital data receiver. The method comprises partitioning the data stream into a plurality of successive data blocks, <u>wherein the size of each successive data block is variable, based on an average size and based on a randomly generated offset</u>. Independent Claim 20 stands finally rejected as being anticipated by Warren however there is no indication in the office action to support such rejection and thus most certainly the Office Action has failed to establish a prima facie case of anticipation of this claim by Warren. It is difficult for applicant to frame a reply to answer the rejection of this independent claim and the claims dependent therefrom when no reasons are provided by the Office Action in support of the rejection.

Independent Claim 28 is directed to a method for the secure transfer of a digital motion image data stream from a digital source to a digital data receiver. This claim also features the step of generating a synchronization index that associates each digital motion image data block with each distinct encryption key. Based on the Office Action's comments vis-à-vis Claim 1 it is assumed that the rejection of Claim 28 as being anticipated by Warren is based on the disclosure of Warren using the various tags which he employs to prevent reproduction. However, these tags are not a synchronizing index that associates each digital image motion data block with a distinct encryption key as called for in Claim 28. As noted in applicant's arguments with regard to Claim 1, the tags of Warren are independent of the encryption keys since they are present and are used for the same purpose in embodiments which do not use encryption keys. They thus perform no function equivalent to that of a synchronization index that associates each digital motion image data block with a distinct encryption key. It is submitted therefore that the Office Action has failed to set forth a prima facie case of anticipation of independent Claim 28 by Warren.

Claim 29 is a dependent claim 28 and recites the step of generating an offset value that is used to establish a starting frame for each digital motion image data block. There is no discussion by the Office Action as to why this claim is anticipated by Warren which provides no disclosure of this feature. It is submitted therefore that the Office Action has failed to set forth a prima facie case of anticipation of dependent Claim 29 by Warren.

Claim 36 is directed to a method for mapping a plurality of encryption keys to a corresponding plurality of encrypted data blocks. The method comprises the steps of providing said plurality of encryption keys separately from said encrypted data blocks; and providing an identifier that correlates a mapping algorithm to said plurality of encryption keys. The Office Action has provided no discussion relative to why this claim is anticipated by Warren and has thus therefore failed to set forth a prima facie case of anticipation of this claim. There is no teaching in Warren or the other prior art of record of providing an identifier that correlates a mapping algorithm to the plurality of encryption keys.

In the rejection of Claim 38 which is a dependent claim of claim 36 the Office Action has attempted to find an isolated teaching in Warren directed to one aspect of the combination which claim 38 represents without identifying how claim 38 in total is anticipated by Warren. It is therefore submitted that the Office Action has also failed to set forth a prima facie case of anticipation of claim 38 or of any claim dependent upon claim 36.

Dependent claims 11 and 14 stand finally rejected as being obvious in view of Warren taken with Handelman. This rejection is also respectfully traversed. Claim 11 is a dependent claim of Claim 1 and adds the feature of the block synchronization data channel utilizes a smart card. Claim 14 is a dependent claim of Claim 1 and adds the feature wherein the key transmission channel utilizes a smart card. Handelman is cited for the disclosure that video data is accessed using a smart card. However, there is no indication in Handelman or in Warren or in their combination of the feature of Claim 1 of providing a block synchronization index indicating a correspondence between the encryption key and the single data block. The Office Action reiterates the teaching of Warren regarding tags which has been shown not to be an index indicating a correspondence between the encryption key and the data block but rather another signal that is totally independent of an encryption key as it is used precisely in the same way in embodiments which do not employ encryption keys. For this reason it is respectfully submitted that the Office Action has failed to set forth a prima facie case of obviousness of Claims 11 and 14.

Claim 19 is a dependent claim of Claim 18 which in turn is dependent upon Claim 1. Claim 19 stands finally rejected as being unpatentable over the combination of Warren in view of Schneier. Schneier provides discussion of linear feedback shift registers for use in cryptography. However, there is no discussion in Schneier regarding the provision of Claim 1 of a block synchronization index indicating a correspondence between the encryption key and the single data block. As has been shown above by applicant there is also no teaching of this feature in Warren. For this reason it is submitted that the Office Action has failed to establish a prima facie case of obviousness of Claim 19.

Claims 42, 45, 46, 50, 53-56 stand finally rejected as being obvious in view of Warren taken with Chaum. Chaum is cited by the Office Action as providing a copy protection system that utilizes two video parts in combination at projection to view the film. Claims 42, 45 and 46 are ultimately dependent upon independent Claim 36. Independent Claim 36 is directed to a method for mapping a plurality of encryption keys to a corresponding plurality of encrypted data blocks that includes the steps of providing the plurality of encryption keys separately from the encrypted data blocks and providing an identifier that correlates a mapping algorithm to the plurality of encryption keys. The Office Action's arguments pertaining to the applicability of Warren concerning Claims 42, 45 and 46 fail to take into consideration the subject matter of Claim 36. Chaum is directed to providing separate components of a video film to make it more difficult to copy the film. Only at the projection of the image are the two parts of the film made visible. There is no discussion in Chaum of the subject matter of Claim 36 nor is there any teaching or suggestion in Warren of this feature either. For this reason it is respectfully submitted that the Office Action has failed to set forth a prima facie case of obviousness of claims 42, 45 and 46.

Claim 47 as amended herein incorporates the subject matter of canceled claims 59 and 60 and is directed to a method of decrypting encrypted digital motion image data blocks of a motion picture comprising providing digital motion image data of a digital motion picture as digital motion image data blocks at least some of which digital motion image data blocks are of different sizes in terms of numbers of frames of said motion picture; and generating a corresponding key from a plurality of encryption keys for use in decrypting a respective digital motion image data block wherein the said at least some digital motion image data blocks each represents plural frames of the motion picture. It is respectfully submitted that the subject matter of Claim 47 is patentable over the prior art cited by the Office Action particularly Warren and Shukla. Shukla as noted by the Office Action discloses that transmission of data blocks can be changed. However, there is no suggestion in Shukla that such change would occur within a particular type of document and particularly to changing within encryption of a single motion picture. The system of Shukla appears to be amenable to change but no indication or reason is provided as to why one would want to change within a particular motion picture. The Office Action appears to be using the applicant's specification in order to reinterpret this reference in the manner not suggested by the specific description in this reference. As noted by the Office Action, Warren also fails to suggest the use of different sizes of numbers of frames for use in encryption of a motion picture. For this reason it is submitted that Claim 47 and claims that are dependent therefrom are patentable over the prior art.

Claim 52 has been rewritten in independent form in view of the amendment of independent Claim 47 from which it originally depended and is directed to a method of decrypting encrypted digital motion image data blocks of a motion picture comprising providing digital motion image data of a digital motion picture as digital motion image data blocks, wherein the digital motion image data blocks are compressed using an MPEG type of compression to form intra-coded stand alone frames and dependent P and B frames, and the intra- coded and P and B frames are encrypted; and generating a corresponding key from a plurality of encryption keys for use in decrypting a digital motion image data block that is encrypted. The Office Action rejected Claim 52 as being anticipated by Warren in that Warren teaches MPEG compression methods. However, there is no disclosure of the type of frames set forth in Claim 52 in the disclosure of Warren. For this reason it is respectfully submitted that the Office Action has failed to set forth a prima facie case of anticipation of Claim 52.

Claim 53 has also been rewritten in independent form in view of the amendment of dependent Claim 47 from which it originally depended. Claim 53 is directed to a method of decrypting encrypted digital motion image data blocks of a motion picture comprising providing digital motion image data of a digital motion picture as digital motion image data blocks, wherein a digital motion image data frame comprises plural color components <u>and only data of one of the color components is encrypted</u>; and generating a corresponding key from a plurality of encryption keys for use in decrypting a digital motion image data block that is encrypted. As the Office Action has noted Warren does not disclose that the video signal is encrypted based on color data. The Office Action notes that Chaum discloses that rather than performing frame by frame protection of the film, protection can be preformed on a color basis. Specifically Chaum describes that a portion of a frame image that is black may be the subject of a second supplementary film portion that is combined with the main portion during projection. However, there is no teaching whatsoever in Chaum regarding encryption on a color basis. It is therefore submitted that the Office Action has failed to establish a prima facie case of obviousness of Claim 53.

<u>CONCLUSION</u>

Dependent claims not specifically addressed add additional limitations to the independent claims, which have been distinguished from the prior art and are therefore also patentable.

In conclusion, none of the prior art cited by the Office Action discloses the limitations of the claims of the present invention, either individually or in combination. Therefore, it is believed that the claims are allowable.

If the Examiner is of the opinion that additional modifications to the claims are necessary to place the application in condition for allowance, he is invited to contact Applicant's attorney at the number listed below for a telephone interview and Examiner's amendment. Alternatively, in view of the failure by the Examiner to properly address the patentability of a number of claims it is requested that the final rejection be withdrawn and a new, non-final, office action be provided to enable applicant to properly respond to the Examiner's arguments for unpatentability.

Respectfully submitted,

Attorney for Applicant(s)
Registration No. 29,134

Nelson A. Blish/tmp
Rochester, NY 14650
Telephone: 585-588-2720
Facsimile: 585-477-4646

If the Examiner is unable to reach the Applicant(s) Attorney at the telephone number provided, the Examiner is requested to communicate with Eastman Kodak Company Patent Operations at (585) 477-4656.